

United States District Court

EASTERN DISTRICT OF OKLAHOMA

In the matter of the search of:

A Silver Honda Accord Crosstour,
Oklahoma tag QWG046, located at 100
South Church Street, Poteau, OK 74953

Case No. 25-MJ-227-JAR

APPLICATION FOR SEARCH WARRANT

I, Brett J. Collins, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the EASTERN District of OKLAHOMA (identify the person or describe property to be searched and give its location):

SEE ATTACHMENT "A"

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

SEE ATTACHMENT "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18, United States Code, Sections 2252 and 2252A, and the application is based on these facts:

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to :

Date: 6/25/2025

City and state: Muskogee, Oklahoma




BRETT J. COLLINS, SPECIAL AGENT
FBI



Judge's signature
JASON A. ROBERTSON
UNITED STATES MAGISTRATE JUDGE

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brett J. Collins, a Special Agent with the Federal Bureau of Investigation (FBI), Oklahoma City Division, Fort Smith Resident Agency, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since 2017. I am currently assigned to the Safe Trails Task Force of the Oklahoma City Division of the FBI. During my time as a Special Agent with the FBI, I have participated in violent crime, organized crime, crimes against children, and drug investigations as the primary investigator or in a subsidiary role. I am familiar with the procedures, activities, and investigative techniques associated with these types of investigations. I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media including computer media. I have participated in investigations of persons suspected of violating federal child pornography laws, including Title 18, United States Code, Sections 2251 and 2252.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and am a “federal law enforcement officer” within the meaning of Fed. R. Crim. P. 41(a)(2)(C).

3. This affidavit is being made in support of an application for a search warrant for a Silver Honda Accord Crosstour, Oklahoma tag QWG046 (the “TARGET VEHICLE”), operated by BRIAN COLLINS GRAHAM, for electronic storage devices located therein, for evidence of violations of Title 18 U.S.C. Sections 2252 and 2252A.

4. The statements in this Affidavit are based in part on my investigation of this matter and on information provided by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are

necessary to establish probable cause to believe that evidence of violations of Title 18 U.S.C. Sections 2252 and 2252A is located in the TARGET VEHICLE.

5. The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations of Title 18 U.S.C. Sections 2252 and 2252A which make it a crime to distribute, transport, receive, possess, or access with the intent to view child pornography or visual depictions of minors engaging in sexually explicit conduct, and any attempts to do so.

6. In summary, the following facts establish that there is probable cause to believe GRAHAM did possess and transport, or attempted to possess or transport, child pornography, that is files depicting minors engaging in sexually explicit activity, and that evidence of these crimes will be located in medium maintained in the TARGET VEHICLE, as further described in Attachment A.

LEGAL AUTHORITY

7. Title 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct, or produced using a minor engaged in such conduct, when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce, and any attempts to do so.

8. Title 18 U.S.C. § 2252A(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in Title 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such child

pornography was produced using materials that had traveled in interstate or foreign commerce, and any attempts to do so.

DEFINITIONS

9. The following definitions apply to this Affidavit:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see Title 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. (See Title 18 U.S.C. § 2256(5)).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. (See Title 18 U.S.C. § 2256(2)).

e. "Computer," as used herein, is defined pursuant to Title 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data

processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Minor" means any person under the age of eighteen years. (See Title 18 U.S.C. § 2256(1)).

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e mail address," an e mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet

Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

i. "Electronic Communication Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. (See Title 18 U.S.C. § 2510(15)).

j. "Hash Value" is a mathematical value generated by applying an algorithm to a computer file that is represented by a sequence of hexadecimal digits. Among computer forensics professionals, a hash value is generally considered to be a unique signature or fingerprint for a file.

BACKGROUND REGARDING COMPUTER/ELECTRONIC DEVICES AND THE INTERNET

10. I have had both on the job training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Cell phones and more advanced devices known as “smart phones” function the same as computers and can run computer software and applications, create and edit files, go on the Internet, chat, text, email, and interact with others on the Internet, and store, send, and receive files, among other functions. Cell phones and smart phones have been used by child pornographers to send, receive, store, and produce images depicting child pornography, as well as engage in voice, email, text, and real time chat conversations with minors and others. Cell phones and smart phones can contain SD cards and/or SIM cards that can store data such as pictures, videos, text messages, contact lists, call logs and other data.

d. GPS, or Global Positioning System, devices can be portable devices used to obtain directions to destinations or show roads and directions in a given area. GPS devices can store the route an individual traveled. GPS devices have been used by individuals to obtain directions when they travel to meet a minor for sexual purposes.

e. Child pornographers can convert photographs into a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer

protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

f. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

g. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

h. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Google, Yahoo!, Hotmail, Sky Drive or One Drive, and Dropbox among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or device, such as a cell phone or "smart phone", with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer devices in most cases.

i. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained

unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO EXHIBIT A SEXUAL INTEREST IN CHILDREN AND INDIVIDUALS WHO DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

11. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. Such individuals who collect child pornography may collect explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals may also collect child erotica, which may consist of images or text that do not rise to the level of child pornography, but which nonetheless fuel their sexual fantasies involving children.

c. Such individuals who collect child pornography may often seek out like-minded individuals, either in person or via the Internet, to share information and trade

depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer, e-mail, bulletin boards, internet relay chat, newsgroups, instant messaging, and other similar vehicles.

d. Such individuals who collect child pornography may maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. Such individuals who collect child pornography often may collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or on scraps of paper.

f. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and damage. However, some individuals may dispose of their collection of their sexually explicit materials or only seek them out when they want to view them in order to conceal their activities for fear of being caught.

g. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on

their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

h. Based on my training and experience and speaking with other law enforcement officers, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences.

i. Importantly, evidence of child pornography, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

BACKGROUND OF THE INVESTIGATION

12. In 2007, GRAHAM was convicted on child sexual abuse charges and sentenced to 10 years in prison. The offense involved GRAHAM, a church employee/volunteer, perpetrating acts of sexual abuse on a 14-year-old boy who attended church where GRAHAM worked.

13. While incarcerated in Arkansas, GRAHAM participated in sex offender community notification assessments. During GRAHAM's 2015 re-assessment, GRAHAM stated that in the past, he masturbated almost exclusively to thoughts of teenage males, from ages 14 to 16. GRAHAM stated he had viewed, but was not sexually aroused by, nude pictures of pre-pubescent or pubescent children. GRAHAM stated he viewed and was sexually aroused by pictures of nude teenagers.

14. Following GRAHAM's release from prison, GRAHAM registered as a sex offender with the Oklahoma Department of Corrections ("ODOC"). As part of the requirements of the Sex Offenders Registration Act, GRAHAM is required to verify his physical address.

GRAHAM listed a residence in Spiro, Oklahoma as his residence beginning on or around June 20, 2016. GRAHAM listed an address in Arkansas as his residence for short periods in 2017 and 2018, however GRAHAM has listed the residence in Spiro as his only residence since on or around December 19, 2018. GRAHAM is required to verify his address every 90 days. GRAHAM last verified his address in April 2025. Additionally, the residence in Spiro is listed as GRAHAM's residential address on his Oklahoma driver's license.

15. In February 2025, I received an investigative lead from the FBI's Child Exploitation Operational Unit ("CEOU"). The information provided in the lead detailed that Coinbase¹ contacted the FBI with information regarding one of their users, GRAHAM, who utilized his Coinbase account to attempt to purchase child sexual abuse material ("CSAM") in 2024. Specifically, on October 26, 2024, GRAHAM's Coinbase account showed two attempted transactions of Bitcoin to Bitcoin address 3N1JgRGywo2PqfmByuMbEHrwHgjKDEcqVZ ("3N1JgRG"). Based on information provided by CEOU, this Bitcoin address (3N1JgRG) was linked to the following CSAM site:

Website IP Address: 127.0.0.1

Website URL:

hxxp://boyssuzjzshvpgirobugqc3tymcug7mnimh2dg2xuk7cvvelbhbakwid.onion

Virtual Currency: Virtual Currency

Bitcoin: 3N1JgRGywo2PqfmByuMbEHrwHgjKDEcqVZ

16. On February 19, 2025, an FBI Special Agent visited the .onion address provided above and confirmed the site was active, and was named, "Boys Asylum." The FBI Special Agent noted the site contained CSAM and a Bitcoin address to pay for access. The Bitcoin address is the same address GRAHAM used when he attempted to pay twice on October 26, 2024. Based on information provided by CEOU, these two payments were not processed by Coinbase because the

¹ Coinbase is a digital currency exchange that allows users to buy, sell, and store cryptocurrencies like Bitcoin and Ethereum. Coinbase is considered one of the most popular platforms for buying and selling crypto.

3N1JgRG address was a blacklisted address due to its labeling of CSAM.

17. The following information was provided by an FBI Forensic Accountant that further analyzed GRAHAM's Coinbase records. In addition to the two blocked payments, there were other indicators of CSAM purchases in GRAHAM's Coinbase account. For example, starting on May 4, 2021, through June 28, 2023, there are monthly payments made from GRAHAM's Coinbase account to a specific Bitcoin address (1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar) with text listed in the "notes" column. Based on the forensic accountant's training and experience and conversations with Coinbase investigators, the "notes" column in the Coinbase records refers to notes that the user puts in the payments.

18. The notes below commonly say "1 mth of VIP" and "1 mth of A51." Based on the forensic accountant's training and experience, they know that CSAM sites often have a VIP area where users can pay for access to more expensive and/or different types of CSAM than the regular access to that CSAM site offers. The amounts paid per month for these subscriptions are often around \$50 - \$60 worth of Bitcoin.

TIMESTAMP	AMOUNT	EQUIV USD	CURRENCY	TO	NOTES
5/4/2021 6:16	(0.001137)	\$ (63.78)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth VIP and 1 mth A51
6/4/2021 20:06	(0.001663)	\$ (62.71)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth VIP and 1 mth a51
7/5/2021 22:24	(0.001727)	\$ (60.02)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 month of VIP and 1 month of A51
8/7/2021 12:48	(0.001301)	\$ (56.61)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	
9/9/2021 13:30	(0.001253)	\$ (57.87)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A%!
10/10/2021 12:20	(0.001005)	\$ (55.55)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51
11/11/2021 15:51	(0.000903)	\$ (58.56)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51
12/13/2021 17:22	(0.001203)	\$ (56.50)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth VIP and 1 mth A51
1/16/2022 6:00	(0.001301)	\$ (56.20)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of Vip and 1 mth of A51
2/19/2022 11:37	(0.001401)	\$ (56.11)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51
3/22/2022 5:48	(0.001359)	\$ (58.23)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51
4/29/2022 12:11	(0.001353)	\$ (52.01)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51 for noble2525
4/30/2022 8:40	(0.000102)	\$ (3.93)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	return password from previous payment on 4/29/22 [URL TRUNCATED] 3A1v55hKkyNw8gcGX1QWxj8xEuU13VYWZf
6/2/2022 19:19	(0.001757)	\$ (53.66)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51
7/4/2022 19:53	(0.002655)	\$ (53.55)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51
8/11/2022 6:30	(0.002128)	\$ (52.41)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51
9/9/2022 13:20	(0.002367)	\$ (50.31)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51
10/12/2022 17:22	(0.002512)	\$ (48.13)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51
11/11/2022 12:29	(0.002930)	\$ (48.71)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51
12/15/2022 19:37	(0.003069)	\$ (53.44)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth VIP and 1 mth A51
1/18/2023 22:54	(0.002617)	\$ (54.54)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	
2/25/2023 17:22	(0.002322)	\$ (53.66)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51
3/23/2023 9:01	(0.002030)	\$ (58.22)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth VIP and 1 mth A51
4/26/2023 7:16	(0.001886)	\$ (56.16)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51
5/28/2023 12:36	(0.001937)	\$ (53.47)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mtn of VIP and 1 mth of A51
6/28/2023 15:59	(0.001858)	\$ (55.95)	BTC	1GEt3ziXvYxEasaTJ5YJLJMKWsh7ToNGar	1 mth of VIP and 1 mth of A51

19. Further review of GRAHAM's Coinbase account showed approximately 60 additional payments of Bitcoin and Litecoin. These payments were most often \$20, or very close to \$20 such as \$19, or \$21, or \$22 worth of Bitcoin or Litecoin. The largest payment made was approximately \$87, the smallest payment was \$7. From the forensic accountant's training and experience, they know that CSAM sold on sites is most commonly between \$20 - \$50 for hundreds of gigabytes, up to around two terabytes.

20. Two of the payments stood out in particular as they match another FBI investigation of a CSAM site called "The Exchange." The Exchange accepts Bitcoin, Litecoin, and Monero from customers. For every \$5 worth of either Bitcoin, Litecoin, or Monero paid in by a customer, their account on The Exchange is credited with 500 tokens. These tokens can be exchanged for CSAM videos. The number of tokens per video varies based on things like quality, duration, and content. Since 2023, the FBI has made several undercover payments to the site. Based on blockchain analysis of those payments, the customer payments are swept out together every couple of days. These customer payments are sent to a relatively non-compliant cryptocurrency exchange called eXch.

21. The same pattern exhibited by The Exchange's sweeps was observed on two of GRAHAM's payments. For example, on November 10, 2023, GRAHAM's Coinbase account sent 0.00061865 BTC (\$23) to Bitcoin address bc1ql5lzcxdg7e0ejqaer75ynvlqy9nmsj7hl2tmv (likely The Exchange's wallet). On November 11, 2023, the wallet containing bc1ql5lzcxdg7e0ejqaer75ynvlqy9nmsj7hl2tmv swept out 88 payments into a deposit at eXch. A review of the 88 payments indicated 13 of them were for around \$5 worth of Bitcoin. Dozens of the other payments were for around \$10, \$20, and \$25, which is consistent with the \$5 per 500 tokens ratio at The Exchange.

22. A few days later, on November 15, 2023, GRAHAM's Coinbase account sent

0.000585 BTC (\$22) to bc1qxdtnssrfzhspaa8wzh2npx8zefcsuaaqfxuzsa (likely The Exchange). An analysis of the wallet containing bc1qxdtnssrfzhspaa8wzh2npx8zefcsuaaqfxuzsa indicated it received a total of 125 other deposits with the same behavior as the other payment GRAHAM made on November 10, 2023. This wallet had two sweeps of the customer payments, both of which went to eXch.

23. GRAHAM's Coinbase account was created on or about March 3, 2021. A review of the subscriber information revealed the following information:

Name: Brian Graham (GRAHAM)
Address: 27257 Tucker Road, Spiro, OK 74959
Phone Number: 501-732-5656

24. In March 2025, Verizon produced subscriber information for telephone number 501-732-5656, the phone number listed on GRAHAM's Coinbase account. A review of the subscriber records revealed GRAHAM is the contact on the account.

25. On or about April 10, 2025, the National Center for Missing and Exploited Children ("NCMEC") received an online cybertip from Robinhood². The tip noted that between January 22, 2025, and March 31, 2025, Robinhood client, GRAHAM, used Robinhood to transfer cryptocurrency to wallets associated with CSAM, totaling \$96.14 via four transfers. A "mobile phone" was listed as the "device used."

26. On June 24, 2025, the LeFlore County Sheriff's Office ("LCSO") contacted GRAHAM on telephone number 501-732-5656, the phone number listed on GRAHAM's Coinbase and Robinhood accounts. The purpose of the call was to schedule GRAHAM to respond to LCSO on June 25, 2025, regarding his sex offender registration.

² Robinhood Markets, Inc. is an American financial services company that provides an electronic trading platform that facilitates trades of stocks, exchange-traded funds, options, index options, futures contracts, outcomes on prediction markets, and cryptocurrency.

27. On June 25, 2025, GRAHAM arrived at LCSO in the TARGET VEHICLE. GRAHAM was subsequently arrested by LCSO personnel. A search of GRAHAM, incident to arrest, was negative for a cellular device. GRAHAM stated his cellphone was located in the TARGET VEHICLE.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER/PHONE SYSTEMS

28. Searches and seizures of evidence from computer devices, cell phones, smart phones, and GPSs commonly require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, cell phones, smart phones, GPSs, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally difficult to accomplish this kind of data search on site; and

b. Searching computer and electronic systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to

tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

29. In addition, there is probable cause to believe that these computer and electronic devices are all instrumentalities of the crime(s), within the meaning of Title 18 U.S.C. §§ 2251 through 2256, and should all be searched and seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

30. To search for electronic data contained in computer, phone, or electronic device hardware, computer, phone, or electronic device software, and/or memory storage devices, the examiners will make every effort to use computer forensic software to have a computer search the digital storage media. This may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. searching for image files to locate images of children engaging in sexually explicit conduct, examining log files associated with the receipt, transmission, and viewing of such images, and examining all of the data contained in such computer hardware, computer software, and /or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. surveying various file directories and the individual files they contain;

c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B;

g. searching for malware in order to evaluate defenses, such as viruses; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

ABILITY TO RETRIEVE DELETED FILES

31. Computer files or remnants of such files on traditional or conventional mechanical computer hard drives can typically be recovered months or even years after they have been downloaded onto the hard drive, deleted or viewed via the Internet. Electronic files downloaded to the hard drive or storage device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a

fixed amount of hard drive space devoted to these files and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from these conventional types of hard drives depends less on when the file was downloaded or viewed than on the particular user's operating system, storage capacity, and computer habits.

32. Other than the conventional mechanical hard drives that are traditionally in computers, becoming more prevalent are flash memory based hard drives and devices. This technology has been traditionally used for small thumb drives where files and data are stored electronically but has since evolved and is being used in computer hard drives known as "solid state hard drives" or SSDs, which are also being used in cell phones and smart phones. These devices do not operate like mechanical hard drives when it comes to how files and data are stored and deleted. These devices can move data around on the drive to maximize storage space and longevity of the drive, compress data, and may use different deletion techniques for how a deleted file is handled and overwritten. Because of how these flash, memory-based drives function it may limit how much data, if any, can be recovered from these types of devices.

Biometric Access to Devices

31. This warrant permits law enforcement to compel GRAHAM to unlock the seized devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

32. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition

features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

33. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

34. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

35. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects

the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

36. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

37. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

38. Due to the foregoing, Affiant requests authorization with this warrant to permit law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of GRAHAM to the fingerprint scanner of the seized devices; (2) hold the seized devices in front of the face of GRAHAM and activate the facial recognition feature; and/or (3) hold the seized devices in front

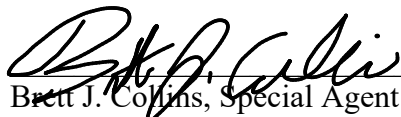
of the face of GRAHAM and activate the iris recognition feature, for the purpose of attempting to unlock the seized devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that GRAHAM state or otherwise provide the password or any other means that may be used to unlock or access the seized devices. Moreover, the proposed warrant does not authorize law enforcement to compel GRAHAM to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the seized devices.

CONCLUSION

39. Based upon the information above I respectfully submit that there is probable cause to believe that violations of Title 18 U.S.C. Sections 2252 and 2252A have been committed and that evidence of those violations is located in GRAHAM's Silver Honda Accord Crosstour, Oklahoma tag QWG046 (the "TARGET VEHICLE"), which is currently parked at the LeFlore County Sheriff's Office parking lot, 100 South Church Street, Poteau, Oklahoma, in the Eastern District of Oklahoma. This evidence, listed in Attachment B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

40. Therefore, I respectfully request that the attached warrant be issued for the location in Attachment A, authorizing the search and seizure of the items listed in Attachment B.

Respectfully submitted,


Brett J. Collins, Special Agent
Federal Bureau of Investigation

Sworn to me this 25th day of June, 2025.



UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Location to be Searched

The property to be searched is a Silver Honda Accord Crosstour, Oklahoma tag QWG046 (the “TARGET VEHICLE”), operated by BRIAN COLLINS GRAHAM. A reference photograph is displayed below:



ATTACHMENT B
ITEMS TO BE SEARCHED FOR AND SEIZED

Evidence of violations of 18 U.S.C. Sections 2251, 2252 and 2252A including the following:

1. All visual depictions of minors engaged in sexually explicit conduct produced using minors engaged in such conduct, on whatever medium (e.g. digital media, optical media, books, magazines, photographs, negatives, videotapes, CDs, DVDs, etc.), including those in opened or unopened e-mails. These include both originals and copies, and authorization is granted to remove videotapes without viewing them at the time and place of seizure, and to view them at a later time.
2. All documents, to include in electronic form, and stored communications including contact information, text messages, call logs, voicemails, Internet searches, photographs, and any other electronic data or other memory features contained in the devices and SIM cards including correspondence, records, opened or unopened e-mails, text messages, chat logs, and Internet history, pertaining to the possession, receipt, access to, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography or minors whether transmitted or received, or which tends to show the knowing possession of any child pornography possessed.
3. All communications and files with or about potential minors involving sexual topics or in an effort to seduce the minor or efforts to meet a minor.
4. All records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider (ISP), cell phone service provider, or electronic service provider, as well as all records relating to the ownership or use of the computer equipment or electronic devices.
5. All records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission in or affecting

interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

6. All records which evidence operation or ownership or use of computer or electronic equipment or devices, including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries, reference materials, or other personal items, and registration information for any software on the computer or device.

8. During the course of the search, photographs of the searched vehicle may also be taken to record the condition thereof and/or the location of items therein.

9. All computer or electronic device passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. Any password or encryption key that may control access to a computer/phone operating system, individual computer/phone files, or other electronic data.

10. Evidence and contents of logs and files on a computer, electronic device, or storage device, such as those generated by the computer's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the computer or device at the time any of the items described in paragraph 1-3 were created, sent, received, or viewed. Also, any malware resident on the computer/phone or device.

11. The following may be seized and searched for all items listed above, and for any items specifically noted in the paragraphs below:

a. Computer hardware, meaning any and all computer equipment. Included within the definition of computer hardware are any electronic devices capable of data processing (such as central processing units, laptop or notebook or netbook or tablet computers, personal digital assistants, gaming consoles, and wireless communication devices to include cellular telephone devices capable of Internet access); peripheral input/output devices (such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media); related communications devices (such as modems, wireless routers, cables and connections, web cameras, microphones); storage media, defined below; and security devices, also defined below.

b. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

c. Computer related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

d. Data security devices, meaning any devices, programs, or data whether themselves in the nature of hardware or software that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer

hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, user names and passwords; data security hardware (such as encryption devices, chips, and circuit boards); data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

e. All storage media capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and backing up electronic data. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer related equipment, such as fixed hard disks, external hard disks, removable hard disks (including micro drives), floppy diskettes, compact disks (CDs), digital video disks (DVDs), tapes, optical storage devices, laser disks, thumb drives, ipods, digital cameras, memory cards (e.g. CF or SD cards), Xboxes, flash drives, or other memory storage devices. This also includes areas with digital storage capability on devices such as printers, scanners, wireless routers, etc.

The above seizure of computer and computer related hardware relates to such computer-related items as being the instrumentalities of crime and also to allow for analysis/search for evidence of crime in an appropriate forensic setting. Upon a determination that such examination would be more appropriately made in a controlled environment, this storage media may be removed and examined at a laboratory location.